«Уязвимости есть всегда»: как орудуют хакеры и что нужно, чтобы от них защититься

Все пользователи заинтересованы в сохранности своих личных данных, однако уровень интернет-безопасности в целом остаётся низким. Мы постоянно слышим о хакерских атаках на крупные организации или же сталкиваемся с махинациями интернет-мошенников в повседневной жизни.
Так возможно ли на сто процентов защититься от угроз киберпреступков, и какие элементарные правила помогут не стать жертвой хакеров?

По мелочи: интернет-мошенники в обычной жизни

Мошенники переводят средства с банковских карт, заражают компьютеры и похищают информацию со смартфонов. Как обезопасить себя от хакеров и возможно ли это вообще?

Компьютер

Первое, что приходит в голову в попытке защитить свой компьютер — установка хорошего антивируса. Выбор антивирусов достаточно широк и становится все более доступным. Так, например, этим летом «Лаборатория Касперского» объявила, что выпускает бесплатную версию своего антивируса.

Но многие пользователи сознательно отказываются от антивирусов, потому что те тормозят компьютер и блокируют атаку там, где ее нет. Ложное срабатывание — нередкое явление. Возможно, вы сами сталкивались с тем, что некоторые сайты считывались вашим антивирусом как вредоносные, хотя на самом деле они были абсолютно безопасны.

В то время как ложные атаки антивирус блокирует, реальную угрозу он может пропустить. Вирусы появляются быстрее, чем антивирусы учатся их определять — иначе бы не существовало хакерских атак. Более того, хакерам иногда даже не обязательно присылать вирус — чтобы получить доступ к конфиденциальным данным пользователя можно прибегнуть к фишингу. Для этого достаточно отправить вам от имени знакомого ссылку на сайт, который выдаёт себя за настоящий, где залогинившись вы сами отдадите доступ.

Чтобы обезопасить свой компьютер от атак, необходимо обновлять операционную систему, не запускать программы из сомнительных источников и внимательно переходить по ссылкам. Также не забывайте делать резервное копирование важных файлов на съемный носитель.

Смартфон

Основной способ взлома смартфона удаленно — это установка самим пользователем вредоносного приложения. Безобидная программа для облегчения жизни или развлечения может оказаться трояном — вредоносным программным обеспечением.

Некоторые трояны **используют уязвимости операционной системы или приложений**, установленных на смартфоне. Подобных атак можно избежать, регулярно обновляя приложения. Дело в том, что разработчики, выпуская обновления, указывают на недочеты и пробелы в предыдущей версии. Эта информация и помогает хакерам сыграть на тех пользователях, которые не успели обновить старую версию.

Вторая группа вредоносных программ вынуждает пользователя **разрешить какие-нибудь действия**, например, доступ к одноразовым паролям из SMS-сообщений, камере или другим приложениям. При загрузке приложения обращайте внимание на то, доступ к какой информации требует предоставить приложение и какие функции вы одобряете.

Для того, чтобы защитить себя от троянов, устанавливайте приложения только из официальных маркетов. Заразиться в Google Play и App Store гораздо сложнее: они проводят проверку приложений, прежде чем открыть доступ пользователям.

Банковская карта

Хищения средств с банковской карты через интернет возможны в нескольких случаях. Например, мошенники могут получить доступ к личному кабинету клиента при помощи сайтов-зеркал (копий настоящих сайтов банков) или вредоносного программного обеспечения. В случае же с мобильным банкингом, как мы писали ранее, на смартфон пользователя загружается вредоносное приложение, с помощью которого мошенники могут через SMS списывать деньги с банковского счета без ведома его законного владельца.

Еще один популярный способ украсть данные о карте — онлайн-шоппинг. При совершении покупок в онлайн-магазинах злоумышленники получают номер карты, срок действия, имя получателя и CVV/ CVC-код.

Единственный способ обезопасить себя от подобных случаев — избегать непроверенных ресурсов для оплаты услуг и всегда внимательно проверять, с каких серверов вы скачиваете ПО или мобильно приложение.

Игра по-крупному: киберпреступность

Кибератаки на различные компании и службы, как и в случае с физическими лицами, совершаются из финансовых побуждений. Иногда хакеры взламывают системы, чтобы получить доступ к какой-либо секретной и уникальной информации, но и это чаще всего является инструментом для вымогания денег.

Последний раз так не повезло американскому каналу HBO: хакерская группировка украла, по их словам, полтора терабайта данных и требовала от канала **выкуп в размере шести миллионов долларов в биткоинах**, угрожая слить всю информацию в общий доступ. В итоге, так и не договорившись с HBO, хакеры выложили в сеть архивы с украденными данными, среди которых были сценарии нескольких серий сериала «Игра престолов», мобильные номера актеров и переписка вице-президента HBO Лесли

Коэн.

Вирус-вымогатель Petya, в июне этого года атаковавший компьютерные системы многих стран, в частности России, Украины, США, а также Индии и Китая, принес хакерам **почти 4 биткоина** (больше 10 тысяч долларов). Атаке [redacted] компьютеры десятков крупных компаний и госструктур — вирус шифровал информацию на жестком диске компьютера, после чего требовал перевести 300 долларов в биткоинах в качестве выкупа за возобновление работы.

В мае этого года по всему миру прошла волна заражений вирусом-шифровальщиком WannaCry. Вирус так же зашифровывал все файлы на компьютере и требовал выкуп в **300 долларов**. В общей сложности, от вируса пострадали около 200 тысяч компьютеров в более чем 100 странах мира, а ущерб от действий хакеров оценили в 1 млрд долларов. В России оказались [redacted] компьютеры Министерства внутренних дел и компании «Мегафон».

Чтобы взломать конкретную инфраструктуру, киберпреступники в течение длительного времени собирают о ней информацию, ищут слабые места в системе безопасности. Чтобы совершить таргетированную (целевую) атаку, хакеры могут пользоваться программными уязвимостями, находя ошибки или недоработки на сайтах. Еще один метод — социальная инженерия: например, сотруднику в социальных сетях добавляется человек под видом старого знакомого или одноклассника и пытается выудить нужную информацию или заставить сделать необходимое действие.

> «Атаки на компании, как правило, не особо отличаются от взлома обычных пользователей: сотрудники фирм так же открывают спам-ссылки. Так что при взломе корпоративных данных во многом играет роль **человеческий фактор**. — говорит ассистент кафедры «Информационная безопасность компьютерных систем» СПбПУ Евгений Павленко. — Полностью гарантировать защиту от мошенников нельзя еще и потому, **что уязвимости есть всегда**. Здесь могут помочь регулярные обновления, антивирусные средства и SIEM-системы *(технология SIEM обеспечивает анализ в реальном времени событий безопасности, исходящих от сетевых устройств и приложений, — прим.)*».

[redacted]

Информационно-аналитический центр